## *REMARKS*

Applicants hereby reply to the Office Action mailed on November 3, 2004. In the above amendments, Applicants now cancel claims 28-31 and add claims 35-37. Applicants respectfully request reconsideration of the pending claims.

CLAIM OBJECTIONS

The Examiner objected to claim 31 under 37 CFR 1.75(c) as being of improper dependent form. Claim 31 has been cancelled as set forth above and the Examiner's objection is now.

REJECTIONS UNDER 35 U.S.C. § 112, ¶ 1

Claims 28-31 stand rejected under 35 U.S.C. § 112, first paragraph, as non-enabling for lack of support in the application for "comparing said signed challenge string and said digital certificate" as recited in claim 28. To expedite prosecution of this application, Applicants cancel claims 28-31 without prejudice or disclaimer, so these rejections are now moot.

In paragraph 7 of the office action, the Examiner rejects claims 18 and 31 under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential steps. The essential element rejection is a non-enablement rejection under 35 U.S.C. § 112, first paragraph. See MPEP § 2172.01. The Examiner, citing the Specification page 21, line 22 to page 22, line 5, asserts that the omitted step is: "creating an authenticated communication channel." Contrary to the Examiner's argument, claim 18 expressly recites "establishing (*i.e.* creating) an authenticated communication channel." To expedite prosecution, claim 31 Applicant cancels claim 31. Accordingly, Examiner's omitted essential step rejections of claim 18 and 31 are moot.

REJECTIONS UNDER 35 U.S.C. § 112, ¶ 2

Claims 18-26 and 28-31 stand rejected as indefinite under 35 U.S.C. § 112, second paragraph, for lack of a description of specific steps as to how the authenticated communication channel is established. Applicants respectfully traverse these rejections. To expedite prosecution of this application, Applicants cancel claims 26, 28-31 without prejudice or disclaimer, so rejections related to these claims are now moot.

Per MPEP 608.01(l), Applicants may rely on the original claims for disclosure of subject matter. Original dependent claim 19 provides exemplary intermediate steps "for establishing an authenticated communication channel comprising . . . embedding an encrypted host system signature in said user's browser; and redirecting said user's browser to said merchant, causing said merchant to authenticate said host system by decrypting said host system signature." Similarly, original dependent claim 20 provides for "establishing an authenticated communication channel [by] communicating a token to said merchant over a first communication channel; receiving a communication from said merchant over a second communication channel requesting said host system to confirm the issuance of said token; and confirming to said merchant that said host system issued said token." Original dependent claims 24-25 likewise provide exemplary steps for establishing an authenticated communication channel.

At least the original claims referenced above provide adequate support for the method step of "establishing an authenticated communication channel" in independent claims 18, 23, and 26. Additionally, the specification further supports with a reasonable degree of particularity and distinctness the term "authenticated communication channel" in the claims. For example, paragraph 12 states:

> [The] authenticated communication channel may be established [using] various cryptographic techniques . . . [in one example] the merchant . . . queries the host system through a second communication channel to confirm the authenticity of the transaction data. Once the communication channel is confirmed [*i.e.*, authenticated], transaction data may be confidently transmitted from the host system to the merchant.

Likewise, paragraph 21 states:

> [T]his communication channel offers increased security, where the merchant 200 is able to verify that the host system 300 sent the number and that the number is appropriately associated with the authenticated user [establishing] a more secure and direct line of communication between the host system 300 and the merchant.

Paragraph 53 further states that "a second communication channel (*e.g.*, a separate http based internet call) to confirm that the host system 300 issued the token . . . via this secure and

authenticated communication channel." Paragraph 54 provides SSL as an exemplary "secure and authenticated channel," and paragraph 61 describes exemplary channels as "a separate internet connection, dedicated connection, and/or the like." Paragraph 62 explains that the "second communication channel [is used] to confirm that the token originated with the host system . . . [*i.e.*, to confirm] the identity of the host system . . . [so that] data may be transmitted more confidently."

Thus, both the original claims and the specification adequately support the method step of establishing an authenticated communication channel. Accordingly, the specification provides adequate disclosure of how to establish an authenticated communication channel rendering claims 18 and 23 sufficiently definite. In light of the amendments and arguments presented and support found in the specification, claims 18, and 23 are sufficiently definite and Applicants request withdrawal of the rejection of theses claims. Similarly, as claims 19-22, and 24-25 variously depend from claims 18 and 23, Applicants submit that these claims are likewise allowable and thus request withdrawal of the rejections of these claims as well.

Claims 28-31 stand rejected as indefinite under 35 U.S.C. § 112, second paragraph, for lack of clarity as to how a "challenge string" provided to a user becomes a "signed challenge string." To expedite prosecution of this application, Applicants cancel claims 28-31 without prejudice or disclaimer, so these rejections are now moot.

The Examiner further rejects claims 28 -31 under 35 U.S.C. 112 as indefinite as to how the system "compare[es] said singed challenge string and said digital certificate." Applicants respectfully traverse these rejections. However, to expedite prosecution of this application, Applicants cancel claims 28-31 without prejudice or estoppel.

REJECTION UNDER 35 U.S.C. § 102

The Examiner rejects claim 26 under 35 U.S.C. § 102(b) as being anticipated by Payne et al., U.S. Patent No. 5,715,314. While Applicants do not acquiesce in the anticipation rejection, Applicants cancel claim 26 as set forth above without prejudice or estoppel to filing one or more applications having claims with similar or identical subject matter. Accordingly, all rejections related to claim 26 are now moot.

REJECTIONS UNDER 35 U.S.C. § 103

Claims 18-25 and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Payne et al. (U.S. Patent No. 5,715,314) in view of Purpura (U.S. Patent No. 6,421,768). Applicants traverse this rejection. To expedite prosecution, Applicants cancel claim 28 as set forth above without prejudice or disclaimer.

Regarding claims 18-22, the Examiner argues that the payment URL hashes disclosed in the Payne reference constitute secondary transaction numbers used to facilitate a transaction. As used in Payne, a hash is typically a data transmission integrity measure or a security tool. For example, a sender generates a hash by applying an algorithm to a text string, and then transmits the hash along with the original text string. Both the text string and hash may be encrypted during transmission. The recipient then decrypts both the message and the hash, produces a second hash from the received original text string, and compares the two hashes to ensure that the message was transmitted intact. At best, the Payne reference teaches the use of a hash of a payment URL purely to ensure the integrity of the transmitted URL. (column 5, lines 26-60; column 7, lines 14-37). The Payne reference is limited to the access URL and the URL hash, and does not teach or suggest the use of a hash to facilitate the submission of a payment request, or the use of a hash to identify a transaction account to be charged in a transaction. Accordingly, the Payne reference does not teach or suggest " communicating said secondary transaction number over said authenticated communication channel to said merchant for use by said merchant in submitting a payment request based on said secondary transaction account number", as recited in independent claim 18.

Accordingly, amended independent claim 18 is patentable over the Payne reference even in view of the Purpura reference. Applicants respectfully request withdrawal of the rejection and consideration of amended claim 18. Similarly, as claims 19-22 depend from claim 18, claims 19-22 are not obvious over Payne in view of Purpura at least for the same reasons as independent claim 18, in addition to their own respective features. Applicants request withdrawal of the rejections and reconsideration of these claims as well.

As per claims 23-25, the Examiner argues that the user ID and password prompts disclosed in the Payne reference constitute automatic recognition of the presence of an

authentication device on a user's computer system. A "device" in the field of computers is any machine or component that connects to a computer (*e.g.*, disk drives, printers, and wireless devices) as opposed to intangible software application features loaded on the computer. See http://www.webopedia.com/TERM/d/device.html. Nothing in the figures or specification passages (figures 1, 4, 7 and 8; column 4, lines 35-37; column 7, lines 31-39; and column 8, lines 33-38) of the Payne reference cited by the Examiner discloses automatically recognizing or detecting the presence of an authentication "device" on a user's computer system. The smart statement documents or smart statement URL authenticator disclosed in Figure 4 and column 8, lines 32-37 of Payne merely relate to "purchase transactions for a given month" with no association to smart cards, smart card readers, or other authentication "devices."

Claim 23, as amended, recites "recognizing the presence of an authentication device on a user's computer system; redirecting said user to a host system website, causing said host system to authenticate said user based on data extracted from a transaction instrument by said authentication device." The specification provides a peripheral smart card reader as one exemplary authentication device on a user's computer system. Nothing in the Payne or Purpura references teaches the automatic recognition of such devices.

Accordingly, amended independent claim 23 is patentable over the Payne reference even in view of the Purpura reference. Applicants respectfully request withdrawal of the rejection and consideration of amended claim 23. Similarly, as claims 24-25 depend from claim 23, claims 24-25 are not obvious over Payne in view of Purpura at least for the same reasons as independent claim 23, in addition to their own respective features. Applicants request withdrawal of the rejections and reconsideration of these claims as well.

Claims 21-22 and 28-31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,715,314 in view of Purpura, U.S. Patent No. 6,421,768 as applied to claim 21 above, and further in view of Gifford, U.S. Patent No. 5,724,424. Applicants traverse these rejections.

As claims 21-22 depend from independent claim 18, claims 21-22 are not obvious over Payne in view of Purpura and further in view of Gifford at least for the same reasons as set forth above to differentiate independent claim 18 from Payne, in addition to their own respective

features. Applicants request withdrawal of the rejections and reconsideration of these claims as well.

Regarding claims 28-31, the Examiner's rejection is now moot since Applicants cancel claims 28-31 to expedite prosecution of this application.

NEW CLAIMS

Applicants add new claims 35-37. As required by 37 C.F.R. 1.111, Applicants assert that new claims 35-37 are specifically distinguished over the applied references for the same reasons as set forth above to differentiate independent claim 18 from Payne. Accordingly, the applied references do not teach or suggest "providing said secondary transaction account number to said merchant for use by said merchant in submitting a payment request based on said secondary transaction account number," as recited in independent claim 35. New claims 36-37 are not obvious over the applied references at least for the same reasons as set forth above to differentiate independent claim 35 from Payne, in addition to their own respective features.

The specification has been amended as set forth above to address the Examiner's previous rejection of claims reciting " comparing said signed challenge string and said digital certificate" (28-31) as recited in new claim 35. This amendment does not constitute new matter as the claim and the amendment are supported by the original specification and claims.

In the Examiner's previous rejection, the Examiner characterized paragraph 54 of the specification as requiring that the digital certificate and signed challenge string be one and the same, implying that they may not, therefore, be compared. The Examiner contends that the disclosure is thus non-enabling. Each of paragraphs 12, 34, 35, and 57 of the specification cited earlier by the Examiner adequately supports the comparison of a signed challenge string and a digital certificate, and examples in which the challenge string and the digital certificate that are to be compared are separate in nature. One of ordinary skill in the art would understand that a "two-factor authentication" involving both a digital certificate and a signed challenge string as described in paragraphs 34 and 35, to mean that each of the two factors are used for authentication by comparison to each other and/or to a third stored data set.

For example, paragraph 34 explains that a digital certificate and signed challenge string are separate parts of a "two-factor authentication employing [a] . . . standard cryptographic

certificate in combination with a PIN." Similarly, paragraph 35 describes the same "two-factor authentication" in terms of:

> [a] microchip 16 [that] stores a digital certificate assigned by the host system . . . the host system [also] sends the user a challenge string . . . When the user 1 enters his or her PIN number the digital certificate is accessed, the challenge string is signed and returned, along with the digital certificate, to the host system.

Paragraphs 12 states that a "user . . . enters an appropriate PIN. The challenge string is signed and transmitted with the digital certificate." (emphasis added). Likewise, paragraph 57 states:

> [The] authentication system . . . obtains a challenge string . . . the user 1 enters the PIN, resulting in the challenge string being signed and returned, with a digital certificate, to the host system . . . [t]he digital certificate and the signed challenge string [are] passed to the user database system. (emphasis added).

In the alternative embodiment described in paragraph 54, in which the merchant system is configured to maintain active control during authentication, a digital certificate is described as but one example of authentication or a signed challenge string. ("A signed challenge string (*e.g.*, digital certificate)"). Paragraph 54 does not require that the signed challenge string and digital certificate be one and the same.

Applicants assert that the specification provides support for comparing a separate signed challenge string and digital certificate and further assert that one of ordinary skill in the art would know how to compare a signed challenge string and a digital certificated to authenticate a user. Nevertheless, in an effort to further prosecution of new claim 35, Applicants also amend the specification as set forth above to more clearly set forth the step of comparing the signed challenge string and digital certificated to authenticate a user.

## CONCLUSION

In view of the above remarks and amendments, Applicants respectfully submit that all of the currently pending claims properly set forth that which Applicants regard as their invention and are allowable over the cited references.

Accordingly, Applicants respectfully request reconsideration and allowance of all pending claims. The Examiner is invited to telephone the undersigned at the Examiner's convenience if the Examiner has any questions regarding this Reply or the present application in general. Applicants authorize and respectfully request that any fees due be charged to Deposit Account No. 19-2814.

Respectfully submitted,

Dated: February 3, 2005

By: Kirk Dorius
Kirk Dorius
Reg. No. 54,073

**SNELL & WILMER L.L.P.**
400 E. Van Buren
One Arizona Center
Phoenix, Arizona 85004
Phone: 602-382-6544
Fax: 602-382-6070
Email: kdorius@swlaw.com